EnCaViBS

WP 2: The NIS Directive and its transposition into national law.

Member State:

Germany

Act to Increase the Security of Information Technology Systems (IT Security Act)

Important notice:

This text is an unofficial translation conducted at the SnT/ University of Luxembourg in the framework of the research project EnCaViBS.

The original legal acts which Member States notified to the European Commission as national execution measures were retrieved from official national databases. In order to focus on the core of the research project, only selected transpositions have been translated.

The translations only serve the purpose of being an information resource; there is no guarantee whatsoever that the translations correctly correspond to the original versions of the laws. Therefore, evidently, the texts have no legal value. The original, as well as the translated version of the legal acts, are available at www.encavibs.uni.lu, where additional information on the research project may be found.

This research project is funded by the Luxembourg National Research Fund (FNR), C18/IS/12639666/EnCaViBS/Cole,

https://www.fnr.lu/projects/the-eu-nis-directive-enhancing-cybersecurity-across-vital-business-sectors-encavibs/.

Fonds National de la Recherche Luxembourg

Member State: Germany

Act to Increase the Security of Information Technology Systems (IT Security Act)

Dated 17 July 2015

The Bundestag passed the following law:

Article 1

Change of the BSI Act

The BSI Act of 14 August 2009 (Federal Law Gazette I p. 2821), which was last amended by Article 3 paragraph 7 of the law of 7 August 2013 (Federal Law Gazette I p. 3154) is changed as follows:

1. § 1 is worded as follows:

   "§ 1 German Federal Office for Information Security
   The Federation shall maintain a Federal Office for Information Security (Federal Office) as superior federal authority. It is responsible for information security on a national level. It is to be overseen by the Federal Ministry of the Interior."

2. The following (10) is added to § 2:

   "Critical infrastructures as referred to in this Act shall mean facilities, equipment or parts thereof which

   1. are part of the sectors energy, information technology and telecommunications, transportation and traffic, health, water, nutrition, and the finance and insurance industries and

   2. are of high importance to the functioning of the community since their failure or impairment would result in material shortages of supply or dangers to public safety. The critical infrastructures as referred to in this Act are defined in detail by the legal regulation pursuant to Section 10 (1)."

3. § 3 is changed as follows:

   a) (1) sentence 2 is changed as follows:

   aa) In number 2, the words "needed to preserve their security interests" are replaced by the words "is needed, as well as for third parties, insofar as this is necessary to preserve their security interests".

bb) In number 15, the words “critical information infrastructures” are replaced by the words “security in information technology of critical infrastructures” and the full stop at end is replaced with a semicolon.

cc) The following numbers 16 and 17 are added:

“16. tasks as central body for the security of information technology with regard to the cooperation with foreign competent bodies, without prejudice to special competences of other bodies;

17. tasks in accordance with Sections 8a to 8c as central body for the security of information technology of critical infrastructures and digital services.”

b) The following section 3 is added:

“(3) The Federal Office may advise and support operators of critical infrastructures in securing their information technology upon their request or refer them to qualified providers of security services.”

4. The heading of § 4 is changed to:

“Central Reporting Office for the Security of Information Technology of the Federation”

4a. § 5 (1) is changed as follows:

a) Sentence 4 is worded as follows:

“The federal authorities shall be obliged to support the Federal Office regarding the measures specified in the first sentence and, while doing so, ensure that the Federal Office has access to internal protocol data of the authorities in accordance with the first sentence no. 1 and interface data in accordance with the first sentence 1 no. 2.”

b) The following sentence is added:

“Protocol data of federal courts may only be gathered with their approval.”

5. § 7(1) sentence 1 will be replaced by the following:

“To fulfil its tasks under § 3 (1) second sentence no. 14, the Federal Office may

1. issue the following warning to the public or affected groups:

a) warnings relating to security gaps in information technology products and services,

b) warnings relating to harmful software and

c) warnings in the event of loss of data or unauthorized access to data;

2. recommend security measures and the use of certain security products.

To fulfil its tasks under the first sentence, the Federal Office may involve third parties, if this is required for an effective warning in due time.”

6. Subsequent to § 7, the following § 7a is added:

"§ 7a

Examination of Security in Information Technology

(1) To fulfil its tasks under § 3 (1) second sentence nos. 1, 14, and 17, the Federal Office may examine information technology products and systems provided on the market or intended to be provided on the market. In doing so, it may use the support of third parties, unless there are conflicting justified interests of the manufacturer of the products and services concerned.

(2) The findings obtained from the examinations may only be used to fulfil the tasks pursuant to § 3 (1) second sentence nos. 1, 14 and 17. The Federal Office may pass on and publish its findings insofar as this is required to fulfil these tasks. Prior to any passing on or publication, the manufacturer of the products and systems concerned shall be given an opportunity to comment subject to an appropriate period."

6a. § 8 (1) is worded as follows:

"(1) The Federal Office shall develop minimum standards for ensuring the security of federal information technology. In consultation with the Council of Chief Information Officers of the federal ministries, the Federal Ministry of the Interior may issue the standards developed in full or in part as general administrative regulations for all federal bodies. The Federal Office shall advise the federal bodies upon request on the implementation of and compliance with the minimum standards. For the courts and constitutional bodies referred to in § 2 (3) second sentence, regulations in accordance with this subsection shall have the status of recommendations."

7. Subsequent to § 8, the following §§ 8a to 8d are added:

"§ 8a

Security Regarding the Information Technology of Critical Infrastructures

(1) Operators of critical infrastructures shall be obliged, within two years from the effective date of the statutory ordinance pursuant to §10 (1) at the latest, to take appropriate organisational and technical precautionary measures in order to avoid disruptions of the availability, integrity, authenticity and confidentiality of their information technology systems, components or processes that are decisive for the functionality of the critical infrastructures operated by them. In doing so, the state of the art shall be observed. Organisational and technical precautionary measures shall be considered appropriate, if the required efforts are not disproportionate to the consequences of a failure or an impairment of the critical infrastructure concerned.

(2) Operators of critical infrastructures and their industry associations may suggest industry-specific security standards for compliance with the requirements according to (1). Upon formal request, the Federal Office shall determine whether these are suitable for complying with the requirements according to (1).

The determination shall be performed

1.in consultation with the Federal Office of Civil Protection and Disaster Assistance,

2.in agreement with the competent federal regulatory authority or in consultation with the otherwise competent regulatory authority.

(3) The operators of critical infrastructures shall appropriately prove compliance with the requirements according to (1) at least every two years. This evidence may be provided by means of security audits, reviews or certifications. The operators shall provide the Federal Office with the results of the audits, reviews or certifications performed including any security deficiencies identified. In the event of security deficiencies, the Federal Office may request:

1. the transfer of the audit, review or certification results and

2. in agreement with the competent federal regulatory authority or in consultation with the otherwise competent regulatory authority, the remedy of the security deficiencies.

(4) Regarding the procedures of a security audit, review and certification according to (3), the Federal Office may define requirements as to the way these are implemented, the proofs to be provided in this regard, as well as the technical and organisational requirements to be met by the auditing body after consultation with representatives of the operators concerned and trade associations concerned.

§ 8b

Central Body for the Security of Information Technology of Critical Infrastructures

(1) The Federal Office shall be the central notification body for operators of critical infrastructures in matters related to the security of information technology.

(2) To perform this task, the Federal Office shall

1.gather and evaluate all relevant information to prevent threats to the security of information technology, in particular information concerning security gaps, malware, successful or attempted attacks on the security of information technology and the observed means used to carry out such attacks,

2.analyse their potential effects on the availability of the critical infrastructures in cooperation with the competent regulatory authorities and the Federal Office of Civil Protection and Disaster Assistance,

3.continuously update the overview of the situation on the security of information technology of the critical infrastructures and

4.immediately inform

a) the operators of critical infrastructures of information concerning them as referred to in nos. 1 to 3,

b) the competent regulatory authorities and otherwise competent federal authorities of the information required to fulfil their tasks under nos. 1 to 3,

c) the competent regulatory authorities of the Länder or the authorities designated for this purpose to the Federal Office by the Länder as central contact points of the information required to fulfil their tasks under nos. 1 to 3.

(3) The operators of critical infrastructures shall specify a contact point for the communication structures under § 3 (1) sentence 2 no. 15 to the Federal Office within six months from the effective date of the statutory ordinance pursuant to § 10 (1). The operators shall ensure that they are

available at any time via this contact point. Information by the Federal Office will be transferred to this contact point.

(4) Operators of critical infrastructures shall immediately notify the Federal Office via the contact point of incidents that have a significant impact on the availability, integrity, authenticity and confidentiality of their information technology systems, components or processes,

1. which may result in a failure or material impairment of the functionality of the critical infrastructures operated by them,

2. which have resulted in a failure or material impairment of the functionality of the critical infrastructures operated by them,

The notification shall include information on the interference, possible cross-border effects and the technical framework, in particular the assumed or actual cause, the information technology concerned, the type of facility or equipment concerned as well as the provided critical service, and the effects of the incident on this service. The identification of the operator shall only be required, if the incident has actually resulted in a failure or an impairment of the functionality of the critical infrastructure.

(5) In addition to their contact point in accordance with (3), operators of critical infrastructures which belong to the same sector may specify a common higher-level point of contact. If such point of contact was specified, information shall, as a rule, be exchanged between the contact points and the Federal Office via the common point of contact.

(6) Where necessary, the Federal Office may request the manufacturer of the information technology products and systems concerned to cooperate in the elimination or prevention of an incident pursuant to subsection 4. Sentence 1 shall apply accordingly to incidents at the premises of operators and permission holders as defined by § 8c (3).

(7) Where personal data is collected, processed or used within the framework of this provision, any processing or use beyond the above mentioned subsections for other purposes shall be impermissible. § 5 (7) sentences 3 to 8 shall be applied accordingly. Furthermore, the regulations of the Federal Data Protection Act shall apply.

§ 8c

Scope of Application

(1) §§ 8a and 8b do not apply to micro enterprises within the meaning of Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124 of 20.05.2003, p. 36). Article 2 (4) of the Recommendation is not applicable.

(2) § 8a is not applicable to

1. operators of critical infrastructures, insofar as they operate a public telecommunications network or publicly available telecommunications service,

2. operators of energy supply networks or energy systems within the meaning of the Energy Industry Act of 07.07.2015 (Federal Law Gazette I p.1970, 3621), as amended by Article 3 of the Law of 17.07.2015 (Federal Law Gazette I p. 1324).

3. permission holders within the meaning of § 7 (1) of the Atomic Energy Act in the version published on 15.07.1985 (Federal Law Gazette I p. 1565), which has been last amended by Article 2 of the Law of 17.07.2015 (Federal Law Gazette I p. 1324), as amended, regarding the scope of application of the permission, as well as

4. further operators of critical infrastructures, insofar as they have to fulfill requirements based on legal provisions that at least correspond with the requirements of § 8a.

(3) § 8b (3) to (5) are not applicable to:

1. operators of critical infrastructures, insofar as they operate a public telecommunications network or publicly available telecommunications service,

2. operators of energy supply networks or energy systems within the meaning of the Energy Industry Act,

3. permission holders within the meaning of § 7(1) of the Atomic Energy Act regarding the scope of application of the permission, as well as

4. further operators of critical infrastructures, insofar as they, based on a legal provision, have to fulfill requirements that at least correspond with the requirements of § 8b (3) to (5).

§ 8d

Request for Information

(1) Upon formal request, the Federal Office may inform third parties about the information obtained within the framework of § 8a (2) and (3) and regarding notifications received under § 8c (4), if legitimate interests of the operator of critical infrastructures do not oppose such requests and the disclosure of information does not interfere with essential security interests. Access to personal data is not granted.

(2) Access to files of the Federal Office in proceedings under §§ 8a and 8b is only granted to parties of the proceedings and pursuant to § 29 of the Administrative Procedures Act."

8. § 10 is changed as follows:

a) (1) will be prepended by the following (1):

"(1) The Federal Ministry of Interior shall determine by means of a statutory ordinance, which does not require the approval of the Bundesrat, after hearing representatives of the scientific community, the operators concerned and the relevant industry associations, in agreement with the Federal Ministry for Economic Affairs and Energy, the Federal Ministry of Justice and Consumer Protection, the Federal Ministry of Finance, the Federal Ministry of Labour and Social Affairs, the Federal Ministry of Food and Agriculture, the Federal Ministry of Health, the Federal Ministry of Transport and

Digital Infrastructure, the Federal Ministry of Defence and the Federal Ministry for the Environment, Nature Conservation, Building and Nuclear Safety, which facilities, systems or parts thereof shall be considered to be critical infrastructures within the meaning of this Act. As regards the latter,

the importance in the respective sectors pursuant to § 2 (10) first sentence no. 2 and their as important considered degree of supply shall be taken into consideration.

The degree of supply to be considered important under sentence 1 shall be determined by means of industry specific threshold values for each service that is considered critical due to its importance in the respective sector.

Access to files relating to the creation or modification of this statutory ordinance shall not be granted."

b) The existing section (1) shall be section (2) from now on and the words "economy and technology by means of statutory ordinance" shall be replaced by "economy and energy by means of statutory ordinance, which does not require the approval of the Bundesrat".

c) The existing section (2) shall be section (3) from now on and in sentence 3 the word "statutory ordinance" shall be followed by a comma and the words "which does not require the approval of the Bundesrat" are added.

9. The following §§ 13 and 14 are added:

"§ 13

Reporting Obligations

(1) The Federal Office shall inform the Federal Ministry of the Interior of its activity.

(2) The information provided under (1) also serves the Federal Ministry of the Interior for informing the public of any danger to the security of information technology which shall be carried out at least once a year by means of a summarising report. § 7 (1) sentences 3 and 4 shall be applied accordingly.

§ 14

Provisions on Fines

(1) It is an administrative offence to willfully or negligently,

1. contrary to § 8a (1) first sentence in conjunction with a statutory ordinance under § 10 (1) first

sentence, fail to take a precautionary measure specified there, to take it improperly, incompletely or not in due time,

2. act in contravention of an enforceable order issued under § 8a (3) fourth sentence,

a) no. 1, or

b) no. 2,

3. contrary to § 8b (3) first sentence in conjunction with a statutory ordinance under § 10 (1)

first sentence, fail to designate a contact point or do so not in due time, or

4. contrary to § 8b (4) first sentence no. 2, fail to submit a report, to submit it improperly, incompletely or not in due time.

(2) In the cases of (1) no. 2 b), the administrative offence may be punished with a fine of up to EUR 100,000.00, in the remaining cases of (1) with a fine of up to EUR 50,000.00.

(3) The administrative authority as defined by § 36 (1) no. 1 of the Code of Administrative Offences shall be the Federal Office."

Article 2

Change of the Atomic Energy Act

[translation omitted]

Article 3

Change of the Energy Industry Act

[translation omitted]

Article 4

Change of the Telemedia Act

[translation omitted]

Article 5

Change of the Telecommunications Act

[translation omitted]

Article 6

Change of the Federal Civil Service Remuneration Act

[translation omitted]

Article 7

Change of the Federal Criminal Police Office Act

[translation omitted]

Article 8

Further Change of the BSI Act

§ 10 (3) BSI Act, last amended by Article 1 of this Act, is abolished.

Article 9

Change of the Act for Structural Reform of the Fees Law of the Federation

[translation omitted]

Article 10

Evaluation

[translation omitted]

Article 11

Entry into Force

This Act will enter into force, subject to sentence 2, on the day following its promulgation. Article 8 enters into force on 14 August 2016.